

CLAIMS:

1. (Original) A method of authenticating a digitally encoded product being originated by an entity having at least one authorized subject, the method including the steps of:

a client system transmitting a request of authentication of the product to a server system,

the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification:

certifying that the product originates from the entity using sensitive information of the entity stored on the server system, and

returning a representation of the certification to the client system.

2. (Original) The method according to claim 1, wherein the step of verifying whether the request is received from an authorized subject includes:

comparing an address of the client system with an indication of authorized addresses stored on the server system.

3. (Original) The method according to claim 1, wherein the step of verifying whether the request is received from an authorized subject includes:

comparing an identifier of a user logged on the client system with an indication of authorized users stored on the server system.

4. (Original) The method according to claim 1, wherein the step of certifying includes:

automatically retrieving a private key of the entity stored on the server system, and

digitally signing the product using the private key.

5. (Original) The method according to claim 4, wherein the step of automatically retrieving the private key includes:

calling a signing command passing a password for accessing the private key as a parameter.

6. (Original) The method according to claim 4, wherein the step of automatically retrieving the private key includes:

calling a signing command with an option causing the import of the private key from a private configuration memory area of the server system.

7. (Original) The method according to claim 1, further including the steps of:

the client system invoking a remote command on the server system, the server system verifying whether the remote command is included in a predefined list stored on the server system, the list including at least one remote command for satisfying the request of authentication, and

the server system executing the remote command if included in the list.

8. (Currently amended) A method of authenticating a software product being originated by an entity having at least one authorized subject, the method including the steps of:

a client system transmitting a request of authentication of the product to a server system,

the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification:

generating a digital signature of the product using a private key of the entity stored on the server system, and

returning the digital signature to the client system, wherein the digital signature certifies that the product originates from the entity.

9. (Original) A computer program directly loadable into a working memory of a data processing structure for performing a method of authenticating a digitally encoded product when the program is run on the structure, the product being originated by an entity having at least one authorized subject, wherein the method includes the steps of:

a client system transmitting a request of authentication of the product to a server system,

the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification:

certifying that the product originates from the entity using sensitive information of the entity stored on the server system, and

returning a representation of the certification to the client system.

10. (Original) A program product comprising a computer readable medium on which a program is stored, the computer program being directly loadable into a working memory of a data processing structure for performing a method of authenticating a digitally encoded product when the program is run on the structure, the product being originated by an entity having at least one authorized subject, wherein the method includes the steps of:

a client system transmitting a request of authentication of the product to a server system,

the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification:

certifying that the product originates from the entity using sensitive information of the entity stored on the server system, and

returning a representation of the certification to the client system.

11. (Original) A computer program directly loadable into a working memory of a client system for performing a method of authenticating a digitally encoded product when the program is run on the client system, the product being originated by an entity having at least one authorized subject, wherein the method includes the steps of:

transmitting a request of authentication of the product to a server system to cause the server system to verify whether the request is received from an authorized subject and to certify that the product originates from the entity using sensitive information of the entity stored on the server system in response to a positive verification, and

receiving a representation of the certification from the server system.

12. (Original) A program product comprising a computer readable medium on which a program is stored, the computer program being directly loadable into a working memory of a client system for performing a method of authenticating a digitally encoded product when the program is run on the client system, the product being originated by an entity having at least one authorized subject, wherein the method includes the steps of:

transmitting a request of authentication of the product to a server system to cause the server system to verify whether the request is received from an authorized subject, and to certify that the product originates from the entity using sensitive information of the entity stored on the server system in response to a positive verification, and

receiving a representation of the certification from the server system.

13. (Original) A computer program directly loadable into a working memory of a server system for performing a method of authenticating a digitally encoded product when the program is run on the server system, the product being originated by an entity having at least one authorized subject, wherein the method includes the steps of:

receiving a request of authentication of the product from a client system, verifying whether the request is received from an authorized subject, and responsive to a positive verification:

certifying that the product originates from the entity using sensitive information of the entity stored on the server system, and

returning a representation of the certification to the client system.

14. (Original) A program product comprising a computer readable medium on which a program is stored, the computer program being directly loadable into a working memory of a server system for performing a method of authenticating a digitally encoded product when the program is run on the server system, the product being originated by an entity having at least one authorized subject, wherein the method includes the steps of:

receiving a request of authentication of the product from a client system,

verifying whether the request is received from an authorized subject, and responsive to a positive verification:

certifying that the product originates from the entity using sensitive information of the entity stored on the server system, and
returning a representation of the certification to the client system.

15. (Original) A data processing structure for authenticating a digitally encoded product being originated by an entity having at least one authorized subject, the structure including at least one client system and at least one server system, wherein each client system has means for transmitting a request of authentication of the product to a server system, and wherein each server system has means for verifying whether the request is received from an authorized subject, and means for certifying that the product originates from the entity using sensitive information of the entity stored on the server system and for returning a representation of the certification to the client system in response to a positive verification.

16. (Original) A data processing structure for authenticating a digitally encoded product being originated by an entity having at least one authorized subject, the structure including at least one client system and at least one server system, wherein each client system has a first software module for transmitting a request of authentication of the product to a server system, and wherein each server system has a second software module for verifying whether the request is received from an authorized subject, and a third software module for certifying that the product originates from the entity using sensitive information of the entity stored on the server system and for returning a representation of the certification to the client system in response to a positive verification.

17. (Currently amended) A data processing structure for authenticating a digitally encoded product being originated by an entity having at least one authorized subject, the structure including at least one client system and at least one server system, wherein each client system has a first software module for transmitting a request of authentication of the product to a server system, and wherein each server system has a second software

module for verifying whether the request is received from an authorized subject, and a third software module for generating a digital signature of the product using a private key of the entity stored on the server system and for returning the digital signature to the client system in response to a positive verification, wherein the digital signature certifies that the product originates from the entity.

18. (Original) In a data processing structure for authenticating a digitally encoded product being originated by an entity having at least one authorized subject, the structure including at least one client system and at least one server system, a client system having means for transmitting a request of authentication of the product to a server system to cause the server system to verify whether the request is received from an authorized subject and to certify that the product originates from the entity using sensitive information of the entity stored on the server system in response to a positive verification, and means for receiving a representation of the certification from the server system.

19. (Original) In a data processing structure for authenticating a digitally encoded product being originated by an entity having at least one authorized subject, the structure including at least one client system and at least one server system, a server system having means for receiving a request of authentication of the product from a client system, means for verifying whether the request is received from an authorized subject, and means for certifying that the product originates from the entity using sensitive information of the entity stored on the server system and for returning a representation of the certification to the client system in response to a positive verification.